Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2021, 8(11):114-122**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

A systematic literature review of Security in Hardware: Hardware Trojans and Countermeasures in Semiconductor Designs

Rajat Suvra Das[1], Shanmugavelan Ramakrishnan[2]

[1]Senior Director, Business Development L&T Technology Services
[2]Director, Cybersecurity Solution Engineering and Customer Success SDG Corporation
Email: rajat.tel@gmail.com, krish.pmo@gmail.com

Abstract The increasing presence of electronic systems in many industries has made the security of hardware components, especially semiconductor designs, a crucial issue. The field of computing hardware has become an appealing target for carrying out potent cross-layer security assaults. These attacks enable hackers to deduce confidential information, seize control over the sequence of operations, undermine the fundamental security measures of a system, pilfer intellectual property, and deceive machine learning algorithms. This study examines the weaknesses in semiconductor designs that are associated with hardware Trojans and suggests innovative solutions to boost integrated circuits' security. The research aims to comprehend the possible risks presented by hardware Trojans, investigate their methods of insertion, and assess the efficacy of existing defenses. Moreover, the study presents novel approaches to enhance the security of semiconductor devices against malevolent hardware intrusions. The results of this Systematic Literature Review (SLR) contribute to a comprehensive knowledge base, providing guidance for future research efforts aimed at improving the security of semiconductor designs in the face of emerging hardware trojan threats.

Keywords Semiconductor Designs; Hardware Trojans; Countermeasures; Security

1. Introduction

During the digital revolution, the increasing dependence on integrated circuits (ICs) has become a defining characteristic of essential systems in several sectors. Integrated circuits are crucial components of contemporary technological infrastructures, spanning industries such as aerospace, healthcare, finance, and communication. Their widespread presence not only demonstrates technical progress but also exposes them to potential risks as they operate in a more intricate environment of threats (Lipp et al., 2018).

Hardware security vulnerabilities may occur at numerous parts of the semiconductor progression, counting specification, production, and recycling (Kocher et al., 2018). They may arise from inadvertent design defects, system repercussions, and deliberate malevolent design alterations (Zhao and Suh, 2018). Typically, their focus is on security assets such as cryptographic functions, along with secure architectures, along with IP, along with ML models. Although traditional hardware security risks like covert along with side channels, along with hardware Trojans, along with reverse engineering continue to evolve, recent attacks have become more powerful by exploiting remote, along with cross-layer, along with specification-compatible attack surfaces. These attacks target strong cryptographic primitives, along with isolation mechanisms, along with memory protection techniques, along with DNNs (Kocher et al., 2018).

Although there are many protective mechanisms available to prevent hardware security concerns, security is still often neglected in the design of hardware. The CVE database is just a small portion of a much larger issue. The

main reason for this is the non-existence of competent hardware safety tools that facilitate automated definition, verification, along with assessment of security restrictions (Ravi et al., 2021).

2. Literature Review

2.1 Hardware Trojans in Semiconductor Designs

Hu et al., (2017), utilized satisfiability to facilitate HT insertion. Also, the Trojan employed a set of indications that, due to route correlation, could not simultaneously reach a specified input combination (logical '0') during normal operation. These signals served as triggers. As a result, the Trojan remained inactive during regular operation, even though each trigger signal had the ability to activate it.Liu et al., (2017), presented a method in which they manipulated the amplitude or frequency of wireless transmission in an analog hardware Trojan (HT) to extract the AES key, while still following the protocol standard. The HT was undetectable via standard testing procedures since it did not alter the functional design.

Antonopoulos et al., (2018), used analog HTs by modifying the dopant polarity or adjusting the input-to-transistor ratio to induce a short circuit. Identifying these high threshold (HT) dopant levels could have been challenging as they didn't add more transistors, but rather altered circuit parameters.

Mahmoud et al., (2020), presented a design for a hardware trojan (HT) by integrating a malicious state into the FSM. The goal was to employ unoccupied state encoding to inject a floating Trojan state. During normal operation, the FSM did not transition to the hanging Trojan state, which was triggered utilising a fault attack, which manipulated the finite state machine to enter a malicious state.

2.2 Current Countermeasures

Alam and Mukhopadhyay, (2019), incorporated a silicon nitride (SiN) layer into a conventional CMOS process to boost the thermal noise to a detectable level without requiring an amplifier. It is worth mentioning that the SiN mask came with a high price tag. In a recent study, introduced a fast True Random Number Generator (TRNG) that utilized the thermal noise straight from the biasing circuit of a common-mode operational comparator along with the sampling uncertainty of a Delay Flip Flop (DFF).

Satpathy et al., (2019), proposed a procedure variation tolerant TRNG by utilizing the collapse of oscillation in a double edge injected Ring Oscillator (RO). To enhance resistance to fluctuations in the manufacturing process, a total of 32 stages were used, with each step offering the flexibility of selecting from 8 different inverters. This approach allowed for a wider range of adjustments and fine-tuning.

3. Methodology

3.1 Search Strategy

- Clearly state the questions that will be the focus on systematic literature review. As an illustration:

1. What kinds of hardware Trojans exist in semiconductor designs, and how do they present themselves?
2. What preventative measures have been suggested to lessen the dangers presented by hardware Trojans?

- Create a search strategy using pertinent terms and phrases pertaining to hardware security, hardware Trojans, semiconductor designs, and countermeasures.
- Identify pertinent databases, journals, and conference proceedings for conducting your literature search

3.2 Inclusion and Exclusion Criteria

- Provide explicit and precise guidelines for determining the criteria used to pick literature, such as the need for peer-reviewed articles, conference papers, and books.
- Indicate the timeframe for publishing in order to concentrate on current advancements.
- Establish explicit exclusion criteria to exclude unnecessary or obsolete material.

3.3 Search Execution

- Implement the search technique across chosen databases, providing thorough coverage.
- Document the quantity of articles and papers first identified.

3.4 Screening Process

- Conduct preliminary evaluation of titles and abstracts to eliminate publications that are not relevant. Conduct a comprehensive examination of items that may be relevant to determine whether they meet the criteria for inclusion.
- Record the reasons for exclusion throughout both phases.

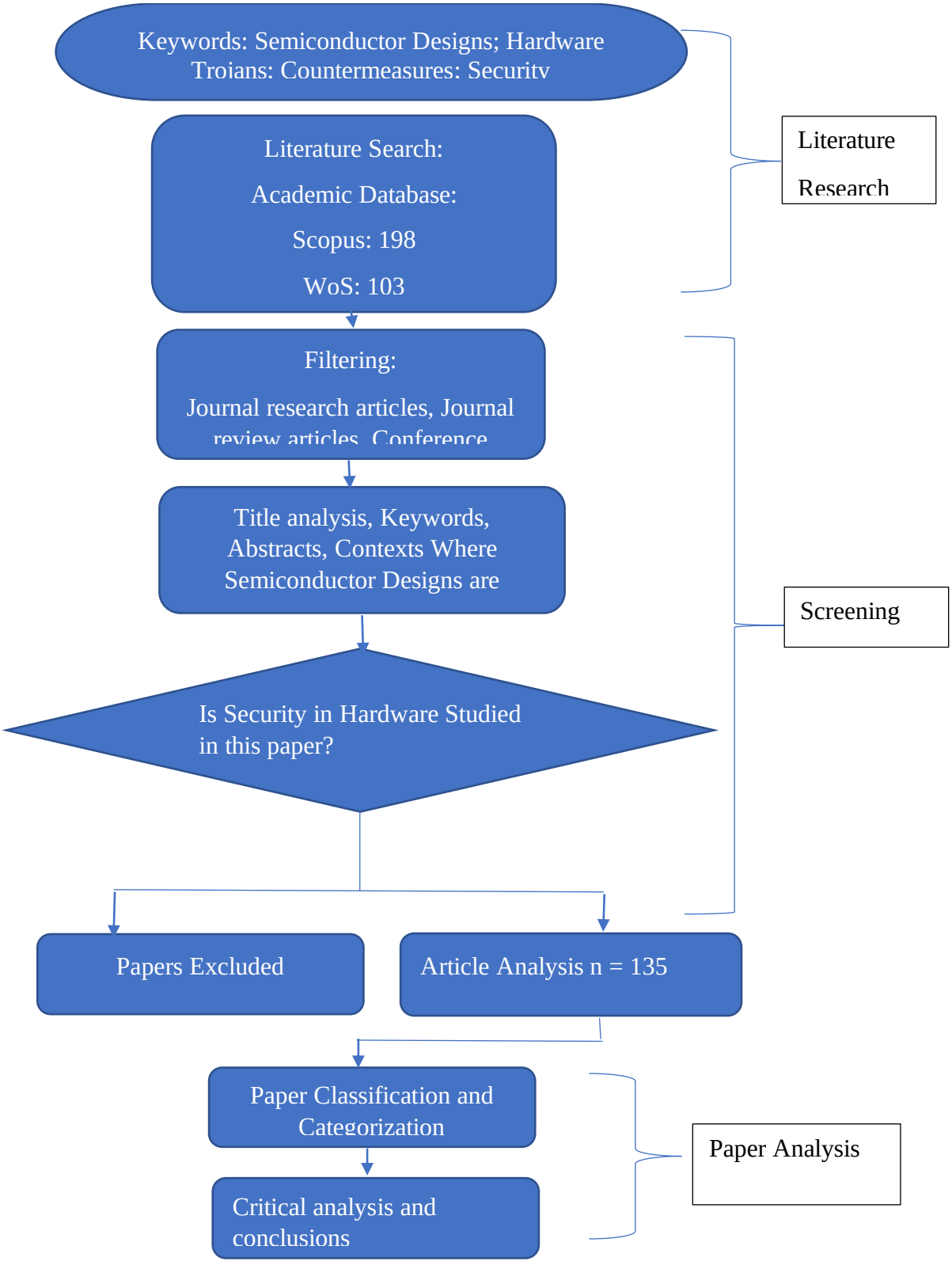

Figure 1: PRISMA flow diagram for the systematic literature

3.5 Vulnerability Analysis

An established vulnerability has been shown in a remarkable manner by the use of adversarial instances.] originally showed that deliberately adding minor perturbations to the original input picture might provide an optical illusion for the DNN classifier during the inference phase.

4.Hardware Trojan Insertion Techniques

4.1 Overview

Hardware Trojans have just lately been the subject of study, resulting in a scarcity of documented implementations. The individuals mentioned in current publications are usually basic, "single hard-coded" solutions that have been exclusively used for the purpose of testing detection and countermeasure verification. Insufficient attention has been devoted to analyzing the comprehensive impact of a solitary or synchronized Hardware Trojan assault, as well as the logistical challenges involved in executing (or identifying) command and control for such attacks.

- Illinois Malicious Processor

  Pathak et al., (2020) uses two versatile strategies for creating malevolent CPUs. The authors demonstrate the feasibility of incorporating Hardware Trojan circuits into a CPU, which may be exploited to carry out various attacks, including password theft, privilege escalation, and unauthorized access to compromised computers. The CPU undergoes two deliberate alterations: the implementation of a memory access mechanism that allows unauthorized access to protected memory areas, and the activation of a shadow mode that enables the execution of concealed "firmware" by an attacker. The authors implemented alterations at the VHDL level and presented results from both simulation and synthesis using a 40MHz Leon 3 SPARC target platform (Zhao et al., 2019).

- Cyber Security Awareness Week

  At the 2008 Cyber Security Awareness Week (CSAW) Embedded System Challenge, which took place at the Polytechnic Institute of NYU, teams were given the challenge of compromising a cryptographic device called "Alpha" that was based on FPGA technology. The objective was to insert a specific set of Trojans into the device without being detected during the validation testing. The teams were given HDL source code and had one month to deliver their concepts (Kundu et al., 2021).

- Pre-silicon Countermeasures:

  Prior to the manufacturing of silicon chips High temperature (HT) detection systems are specifically developed to find and detect high temperatures at the early stages of the design process. Switching probability analysis-based techniques for HT detection are created on the idea that the Trojan trigger signal should have a very low likelihood of switching in order to minimize the frequency of HT activation. These approaches aim to detect signals with switching activity that are considerably below the average by using structure analysis or behavioral code analysis (Haider et al., 2019). Structural checking approaches for HT detection aim to identify certain structural characteristics of HT designs, such as gate type, gate count, and interconnection patterns. These methods use techniques like pattern matching to conduct the detection process. Security verification may be used to identify certain categories of HTs. The process involves developing formal security models for hardware designs and verifying security features, such as confidentiality and integrity, using formal methods such as SAT solving, model checking, and type checking (Mishra et al., 2021).

- Post-silicon Countermeasure:

  Pre-silicon hardware Trojan detection approaches aim to identify any illicit alterations to the chip design after its manufacturing. Destructive reverse engineering (RE), a widely used method for post-silicon high-temperature (HT) detection, entails the removal of packaging and layers from integrated circuits (ICs) and the extraction of circuit structure from layout pictures. Nevertheless, this expensive and labor-intensive procedure may prove ineffective when HT is only included into a limited quantity of chips. In contrast, non-destructive approaches, like as functional testing and SCA, are often seen as more feasible in practical applications (Ardeshiricham et al., 2019). One significant area of study is on developing test vectors that may activate seldom transitioning nodes within a circuit. Statistical methods have offered a potential answer, while another technique involves conducting guided testing against hypothesis tests in crucial parts of the design (Charles and Mishra, 2021). SCA-based techniques identify hardware trojans by examining physical integrated circuit (IC) characteristics, such as power consumption, path latency, and chip emissions. The primary obstacles associated with these approaches are the absence of a reference chip and the impact of process variation on side-channel

data. In order to enhance the sensitivity of HT detection, researchers use various side channel characteristics or integrate logic testing and SCA to generate specific patterns (Huang et al., 2018).

- Design-for-Trust (DFS) Techniques:
  DFS approaches include specialized logic to aid in the discovery of hidden terminals. To expedite the activation phase of a Trojan, several methods include including more fake flip-flops and testing points to enhance the controllability and observability of internal nodes. Another variant of DFS methods involves including circuit components such as ring oscillators and current sensors to aid in the screening and on-site monitoring of chips contaminated with HT, or to enhance the detection of HT by side-channel analysis (Liu et al., 2019).
- Runtime Monitoring Techniques:
  Given the NP completeness of several testing difficulties, including as controllability, observability, and ATPG, it is not feasible to ensure the total elimination of HTs prior to device deployment (Kar et al., 2018). Therefore, it is advantageous to use runtime monitoring methods to identify and thwart HT assaults in systems that are crucial for security (Chakraborty et al., 2020).
- 3PIP Trojan Detection:
  Most HT detection technologies mostly rely on Trojan benchmarks to assess their efficacy. Detecting unknown hidden threats (HTs) in 3PIP is particularly difficult since there is less information available about the specific implementation of the Trojan. The inclusion of functional testing coverage, study of switching probability localization, and the impact of process variation noise contribute to the complexity of this approach. The effectiveness of functional and security verification methodologies is very promising, since the detection rate is contingent upon the quality of the attributes (He et al., 2020).
- HT Prevention Techniques:
  HT preventive approaches attempt to increase the level of difficulty or ideally make the insertion of HT impossible. Logic obfuscation, split manufacturing, and structural obfuscation are three prevalent methods used to avoid the formation of Trojans. The obfuscated circuit's functionality is inaccessible to the untrusted foundry without the appropriate key. HT implantation is a challenging process (Shan et al., 2019). Split Manufacturing may further serve as a preventive measure against malevolent alterations to the design. The design layout is divided into two parts: Front End of Line (FEOL) and Back End of Line (BEOL). These parts are then manufactured by trusted and untrusted foundries, respectively. Lacking knowledge on the back-end-of-line (BEOL) segment, the untrusted foundry has challenges in including a valuable high-throughput (HT) component (Lebedev et al., 2018).

4.2 Case Studies

Suppose an assailant is employed as a design engineer at a chip production plant, as shown in Figure 2, with the intention of altering the chip's functioning upon the occurrence of a certain event. This is a trojan activated by combinational logic, in which setting both A and B to 0 results in an inaccurate value for the output C (C modified). This circuit is designed to identify and prevent an attacker from injecting a trojan, which is a malicious program, based on a rare occurrence. This event is very unlikely to be caught during the testing phase. The figure illustrates the trojan features as follows: change in functionality, combinational, functional, internally triggered, tiny, clustered, and enhanced. These properties are numbered 12, 17, 18, 21, 24, 26, and 27 in R3. Upon analyzing the equivalent columns in R23, it is evident that these characteristics are all closely linked to the development environment inside the abstraction category (attribute 8) (Murdock et al., 2020).

- Combinational Trojan

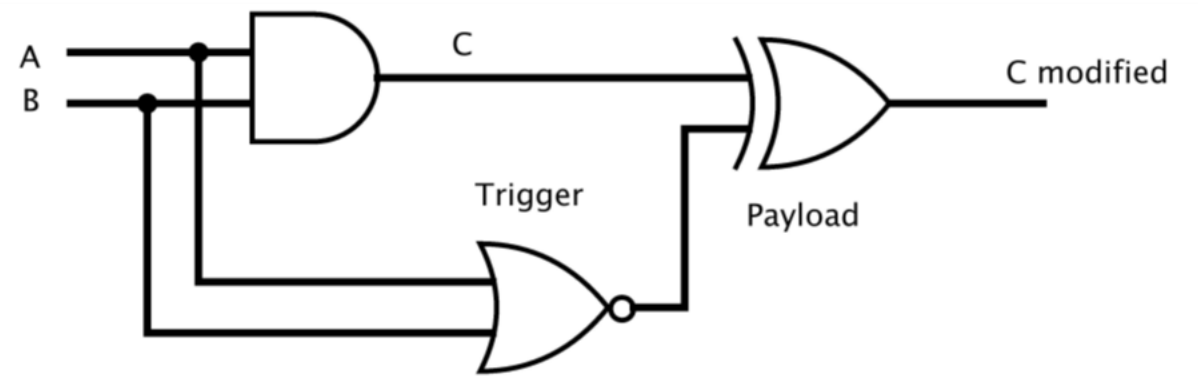

Figure 2: A combinational logic triggered trojan (Murdock et al., 2020)

5. Proposed Countermeasures:

The True Random Number Generator (TRNG) and Physical Unclonable Function (PUF) are two crucial hardware-based security mechanisms that offer inherent protection against emerging threats and vulnerabilities throughout the life cycle and operation of integrated circuits (ICs) or devices. In recent years, PUFs have received much attention from researchers, in contrast to TRNG.

TRNG: A random number generator is a tool or program that produces sequences of unexpected numbers. The traditional methods of using dice roll or coin toss to generate natural randomness are insufficiently expedient to satisfy the requirements of contemporary computer systems. A pseudorandom number generator (PRNG) is a computational procedure or a mathematical equation that may be used to generate a series of integers that seem random, but really follow a deterministic pattern. This sequence has a limited but sufficiently lengthy duration (Koeberl, 2020).

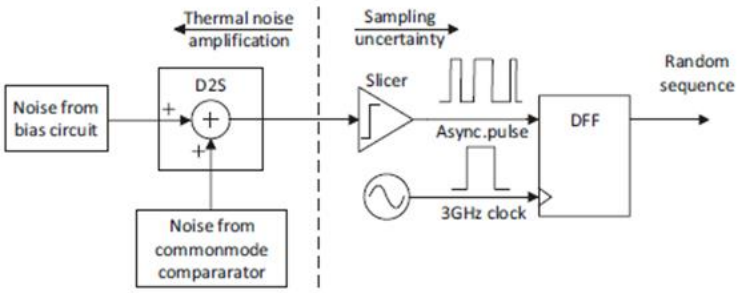

Figure 3: Design concept of noise-based TRNG (Elshamy et al., 2020).

Thermal noise is a reliable source of randomization due to its independence from frequency and technology (Elshamy et al., 2020; Koeberl, 2020). An amplification of the weak thermal noise is required, necessitating the use of a wide-bandwidth amplifier. However, this amplifier may use a substantial amount of silicon area and power. The concept is shown in Figure 3. The act of connecting both inputs of a comparator to the output of a beta-multiplier voltage reference results in the generation of common-mode noise. The thermal noises originating from the comparator and the biasing circuit are combined and then amplified by the differential-to-single ended (D2S) amplifier. The amplified noise is inputted into a slicer to produce a maximum output, which is then sampled by a 3 GHz clocked DFF (Sengupta and Rathor, 2019). This True Random Number Generator (TRNG) achieves a very high data transfer rate of 3 Gbps by effectively using both thermal noise and sampling uncertainty from the asynchronous input. The power consumption of the device is very high, reaching 5 milliwatts, without including the power-demanding external high-speed clock generator (Rajpu and Maniatakos, 2019; Kachave et al., 2018).

6. Evaluation and Results

The SLR revealed a range of vulnerabilities that are inherent in semiconductor designs, serving as possible access sites for hardware Trojan assaults. These vulnerabilities appear at several levels of the hardware system, including architectural, logical, and physical components. Typically recognized areas of concern are supply chain vulnerabilities, vulnerabilities during the design phase, and vulnerabilities arising from the manufacturing process.

- Supply Chain Vulnerabilities:
  The supply chain is a crucial point where semiconductor designs are susceptible to the introduction of hardware Trojans. Sources of risk include counterfeit components, untrustworthy foundries, and hacked third-party intellectual property (IP). The presence of Trojan-infected components throughout the procurement and assembly processes presents substantial risks to the integrity of the final hardware product.
- Design Phase Vulnerabilities:
  The design process is susceptible to vulnerabilities, which might emerge via compromised design tools, insider threats, or inadvertent design defects. Deficiencies in the design process might unintentionally create weaknesses that can be taken advantage of by hardware Trojans. This encompasses the vulnerability to reverse engineering and illegal access that might occur during the design process.
- Significance of Identified Vulnerabilities in the Context of Hardware Trojan Threats:
  Comprehending the importance of these reported weaknesses is crucial in assessing the possible consequences of hardware Trojan attacks on semiconductor architectures. The weaknesses not only provide opportunities for the insertion of Trojans, but also worsen the difficulties in recognizing and managing these attacks.

7. Discussion

The recognition of weaknesses at different phases of the semiconductor lifecycle highlights the need for a comprehensive approach to security. The results imply a need to move away from conventional security paradigms towards more flexible and responsive techniques. Moreover, the study results highlight the interdependence of security measures across the supply chain, design phase, and production processes. Addressing hardware Trojan risks requires a collective approach and shared obligations among stakeholders, such as semiconductor makers, designers, and supply chain partners.

7.1 Potential Challenges and Considerations:

- Complexity of Supply Chain Management: The successful implementation of safe supply chain processes necessitates the harmonious collaboration of many stakeholders, such as suppliers, manufacturers, and distributors. To guarantee the authenticity of components along the supply chain, it is necessary to implement advanced verification procedures and increase transparency. This requires a change in the present practices of supply chain management.
- Integration with Existing Design Processes: Incorporating safe design approaches into current design processes has issues regarding compatibility and flexibility. To mitigate vulnerabilities in the design process, it may be necessary to modify existing procedures and integrate new technologies, which might possibly disrupt present industrial practices.
- Resource Intensiveness of Manufacturing Verification: Ensuring the accuracy and reliability of semiconductor designs throughout the production process requires substantial resources. Integrating tamper-evident methods and rigorous testing protocols might result in higher manufacturing costs and longer lead times, necessitating a careful equilibrium between security and economic factors.

8. Conclusion

Hardware security encompasses many layers of abstraction inside the computer system stack. This article presents a comprehensive examination and analysis of the latest advancements in certain areas of hardware security. This analysis highlights the significant danger that hardware Trojans bring to semiconductor architectures. The study emphasizes the need for comprehensive countermeasure measures to adequately

address the hazards presented by hardware Trojans. In addition to conventional security paradigms, the incorporation of secure design methods, rigorous supply chain management, and thorough production verification are essential elements of a complete protection against these subtle threats. Hardware assaults and responses are advancing quickly. It is expected that each significant shift in processor designs and computing technologies will result in the identification of a distinct shortest bar of the wooden barrel. Consequently, this evaluation serves as a warning to hardware designers and tool developers to provide extra consideration to important security vulnerabilities that cannot be resolved using conventional hardware design and verification methods.

References

[1]. Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., and Hamburg, M. (2018). Meltdown, ArXiv e-prints.

[2]. Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., and Yarom, Y. (2018). Spectre attacks: Exploiting speculative execution, ArXiv e-prints.

[3]. Zhao, M., and Suh, G. E. (2018). FPGA-based remote power side-channel attacks, in IEEE Symp. on Sec. and Priv. (SP), pp. 229–244.

[4]. Ravi, P., Najm, Z., Bhasin, S., Khairallah, M., Gupta, S. S., and Chattopadhyay, A. (2019). Security is an architectural design constraint, Microprocessors and Microsystems, vol. 68, pp. 17–27.

[5]. Mahmoud, D., Hu, W., and Stojilovic, M. (2020). X-attack: Remote activation of satisfiability don't-care hardware trojans on shared fpgas, in Int. Conf. on Field-Programmable Logic and Applications (FPL), p. 8.

[6]. Hu, W., Zhang, L., Ardeshiricham, A., Blackstone, J., Hou, B., Tai, Y., and Kastner, R. (2017). Why you should care about don't cares: Exploiting internal don't care conditions for hardware Trojans, in Int. Conf Comput.-Aided Des. (ICCAD), pp. 707 713.

[7]. Antonopoulos, A., Kapatsori, C., and Makris, Y. (2018). Hardware Trojans in Analog, Mixed-Signal, and RF ICs. Cham: Springer International Publishing, 201. 101–123.

[8]. Liu, Y., Jin, Y., Nosratinia, A., and Makris, Y. (2017). Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs, IEEE Trans. VLSI Syst., vol. 25, no. 4, pp. 1506–1519.

[9]. Alam, M., and Mukhopadhyay, D. (2019). How secure are deep learning algorithms from side-channel based reverse engineering? in Des. Autom. Conf. (DAC), Jun, pp. 1–2.

[10]. Satpathy, S. K., Mathew, S. K., Kumar, Suresh, V., Anders, M. A., Kaul, H., Agarwal, A., Hsu, S., Krishnamurthy, R. K., and De, V. (2019). An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical Von Neumann extraction in 14-nm tri-gate CMOS, IEEE J. Solid-State Circuits, vol. 54, no. 4, pp. 1074–1085.

[11]. Pathak, A.; Saha, P.; Kundu, S. (2020) On Test Generation for Functionally Incomplete Designs. In Proceedings of the 2020 IEEE 29th Asian Test Symposium (ATS), Penang, Malaysia, 23–26; pp. 1–6.

[12]. Kundu, S.; Meng, X.; Basu, K. (2021) Application of Machine Learning in Hardware Trojan Detection. In Proceedings of the 2021 22nd International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 7–9; pp. 414–419.

[13]. Haider, S. K., Jin, C., Ahmad, M., Shila, D. M., Khan, O., and van Dijk, M. (2019). Advancing the state-of-the-art in hardware Trojans detection, IEEE Transactions on Dependable Secure Computing, vol. 16, no. 1, pp. 18–32.

[14]. Mishra, S.K.; Patra, S.K. (2021) Survey of Recent Developments for Hardware Trojan Detection. In Proceedings of the 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Republic of Korea, 22–28.

[15]. Charles, S.; Mishra, P. (2021). A survey of network-on-chip security attacks and countermeasures. ACM Comput. Surv. 2021, 54, 1–36.

[16]. Huang, Y., Bhunia, S., and Mishra, P. (2018). Scalable test generation for Trojan detection using side channel analysis, IEEE Trans. Inf. Forensics Security, vol. 13, no. 11, pp. 2746–2760.

[17]. Liu, Q.; Zhao, P.; Chen, F. (2019). A Hardware Trojan Detection Method Based on Structural Features of Trojan and Host Circuits. IEEE Access, 7, 44632–44644.
[18]. Chakraborty, A., Jayasankaran, N. G. Liu, Y., Rajendran, J., Sinanoglu, O., Srivastava, A., Xie, Y., Yasin, M., and Zuzak, M. (2020). Keynote: A disquisition on logic locking, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 39, no. 10, pp. 1952–1972.
[19]. He, J., Guo, X., Ma, H., Liu, Y., Zhao, Y., and Jin, Y. (2020). Runtime trustevaluation and hardware Trojan detection using on-chip EM sensors,in Des. Autom. Conf. (DAC), pp. 1–6.
[20]. Shan, W., Zhang, S., Xu, J., Lu, M., Shi, L., and Yang, J. (2019). Machine learning assisted side-channel-attack countermeasure and its application on a 28-nm AES circuit, IEEE J. Solid-State Circuits.
[21]. Lebedev, I., Hogan, K., and Devadas, S., (2018). Secure boot and remote attestation in the sanctum processor, in IEEE Computer Security Foundations Symposium (CSF). IEEE, pp. 46–60.
[22]. Murdock, K., Oswald, D., Garcia, F. D., Van, J., Bulck, Gruss, D., and Piessens, F. (2020). Plundervolt: Software-based fault injection attacks against intel SGX, in IEEE Symp. on Sec. and Priv. (SP).
[23]. Elshamy, M., Natale, G. Di., Pavlidis, A., Lou¨erat, M., and Stratigopoulos, H. (2020). Hardware Trojan attacks in analog/mixed-signal ICs via the test access mechanism, in IEEE European Test Symposium (ETS), pp. 1–6.
[24]. Rajput, P. H .N. and Maniatakos, M. (2019). Jtag: A multifaceted tool for cyber security, in IEEE Int. Symp. on On-Line Testing and Robust System Design (IOLTS), pp. 155–158.
[25]. Kachave, D., Sengupta, A., Neema, S., and Sri Harsha, P. (2018). Effect of NBTI stress on DSP cores used in CE devices: threat model and performance estimation," IET Computers Digital Techniques, vol. 12, no. 6, pp. 268– 278.
[26]. Koeberl, P., (2020). Multi-tenant fpga security: Challenges and opportunities, in Int. Symp. on Field-Programmable Gate Arrays. New York, NY, USA: ACM, p. 23.
[27]. Zhao, Y., Hu, X., Li, S., Ye, J., Deng, L., Ji, Y., Xu, J., Wu, D., and Xie, Y. (2019). Memory Trojan attack on neural network accelerators, in Des. Autom. Test Europe Conf. Exhib. (DATE), pp. 1415–1420.
[28]. Ardeshiricham, A., Takashima, Y., Gao, S., and Kastner, R. (2019). VeriSketch: Synthesizing secure hardware designs with timing-sensitive information flow properties, in ACM SIGSAC Conference on Computer and Communications Security, pp. 1623–1638.
[29]. Kar, M., Singh, A., Mathew, S. K., Rajan, A., De, V., and Mukhopadhyay, S. (2018). "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," IEEE Journal of Solid-State Circuits, vol. 53, no. 8, pp. 2399–2414.
[30]. Sengupta, A., and Rathor, M. (2019). Crypto-based dual-phase hardware steganography for securing IP cores, IEEE Letters of the Computer Society, vol. 2, no. 4, pp. 32–35.